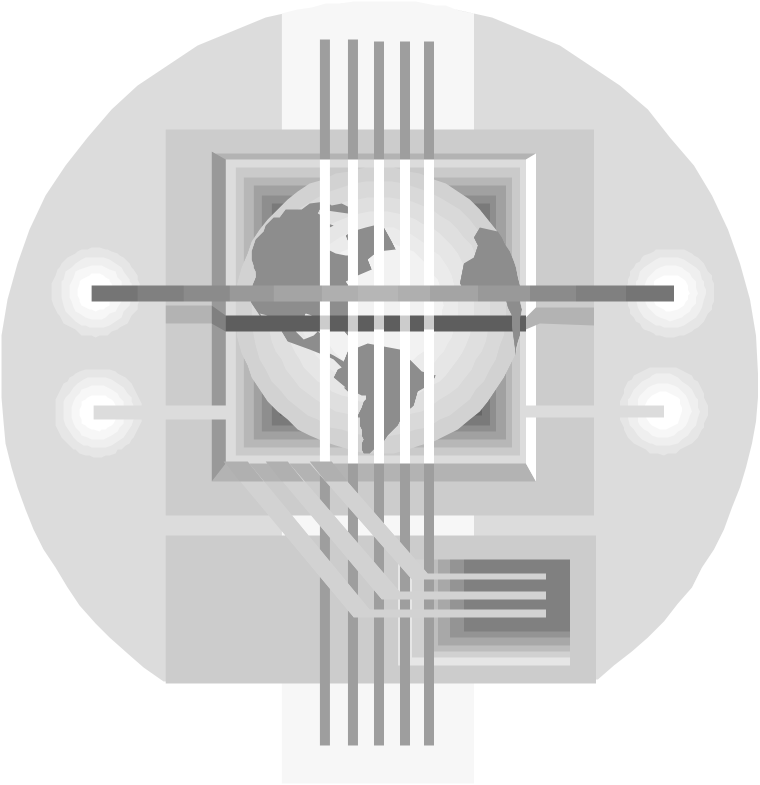
Complex Electronic Hardware Design Assurance Overview RTCA DO-254 / EUROCAE ED-80

Presented for Seattle ACO DER Standardization Seminar, November 4-6, 2003

**Gregg Bartley
FAA Transport Airplane Directorate
Standards Staff, ANM-111
gregg.bartley@faa.gov**

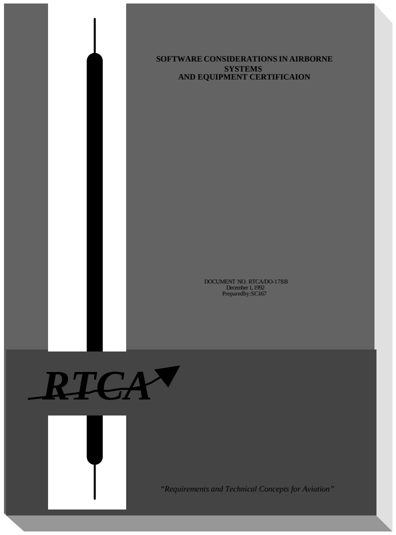


Overview

- Purpose of D0-254
- Summary of contents of D0-254
- Invocation of D0-254
- Future FAA CEH advisory material and guidance
- Differences between D0-178B and D0-254
- Issues
- Summary

DO-254 / ED-80

- Product of Joint RTCA Special Committee 180 and EUROCAE Working Group 46
- Title: “Design Assurance Guidance for Airborne Electronic Hardware”
- Approved in April 2000



SOFTWARE CONSIDERATIONS IN AIRBORNE
SYSTEMS
AND EQUIPMENT CERTIFICAION

DOCUMENT NO. RTCA/DO-178B
December 1, 1992
Preparedby:SC-167

RTCA

“Requirements and Technical Concepts for Aviation”

Purpose of using D0-254 for an Acceptable Means of Compliance

- Inconsistent findings of compliance across projects, due to lack of agreed upon standard.
- No specific guidance for CEH available that can be used to show compliance to FAR XX.1309 regulations.
- Increasing complexity of CEH devices, in many cases, makes exhaustive testing impractical or impossible.
- D0-254/ED-80 is an industry standard, written specifically for CEH, which all participants agreed could and should be used as an Acceptable MOC.
- Following D0-254 minimizes the chance of design error. It does not ensure zero design errors.

Related Regulations and Policy

- FAR/JAR 21, 23.1301, 23.1309, 25.1301, 25.1309, etc.
- AC/AMJ 23/25.1309-1C/1A, etc.
- FAA TAD PLD Issue Paper
- FAA Change Impact Analysis Notice
- Changes: 21.91-.101 (TC), 21.115 (STC), 21.611 (TSO)
- FAA Order 8110.4B, Sec. 14, par. c.
- AC CEH (upcoming)
- Order 8110.CEH (upcoming)
- TAD PLD Policy Statement (upcoming)

DO-254 Outline (1/3)

Foreword

Executive Summary

Membership

- Section 1 Introduction
- 2 System Aspects of Hardware Design Assurance
- 3 Hardware Design Life Cycle
- 4 Planning Process
- 5 Hardware Design Processes

DO-254 Outline (2/3)

- Section 6 Validation & Verification Processes
- 7 CM Process
- 8 Process (Quality) Assurance
- 9 Certification Liaison
- 10 Hardware Design Life Cycle Data
- 11 Additional Considerations

DO-254 Outline (3/3)

- App A Modulation of Data based on Level
- App B Design Assurance for Levels A & B
- App C Glossary
- App D Acronyms

Invocation of D0-254 on certification programs

- There is currently no FAA guidance material that recognizes D0-254 as an Acceptable Means of Compliance.
- In all recent programs for Transport Airplanes, generic Issue Paper “Programmed Logic Devices” has been applied.
  - Invokes D0-254 as an Acceptable MOC.
  - Clarifies definitions and certification requirements for Simple vs. Complex hardware devices.

Future CEH policy and guidance

- Advisory Circular CEH (final number TBD) in final release process.
  - AC invokes D0-254 as an Acceptable Means of Compliance for components containing CEH.
- FAA Order 8100.CEH (final number TBD) will be in work after release of AC.
  - Intent of Order is to clarify issues of scope, applicability, and technical details not covered in AC.
- TAD Policy Memo in work
  - Intended as “Stop Gap” policy until FAA Order is available.

Some Major Differences between D0-254 and D0-178B

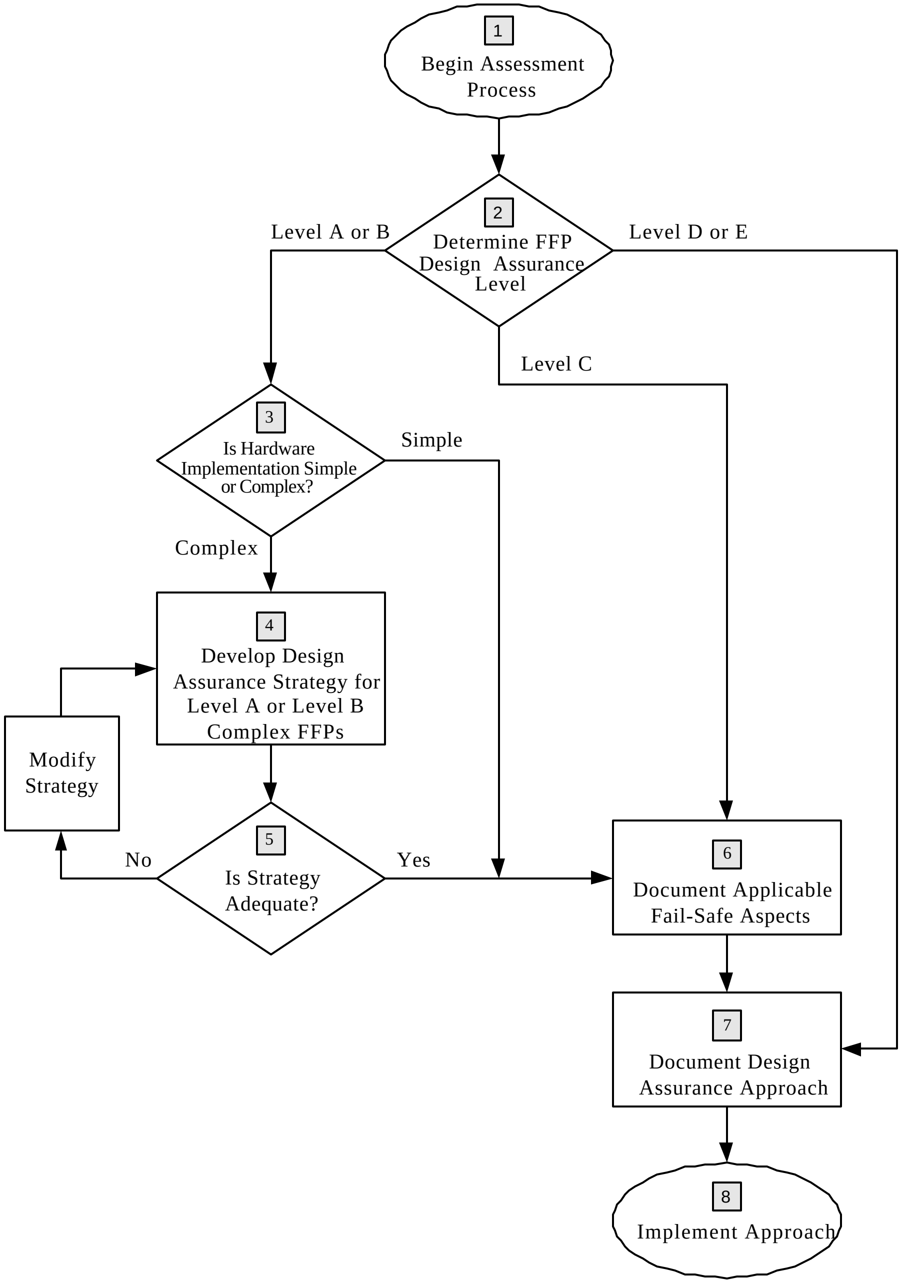
- 1.2 Scope (includes PCB's and LRU's)
- 1.6 Complexity considerations (simple vs. complex hardware)
- Table 2-1 DAL vs. Hazard Classification, "cause a failure" in D0-254 vs. "cause or contribute to a failure" in D0-178B.
- 2.3.1 Allows piece part into single Functional Failure Path in hardware, can be different DAL for each FFP.
- 5.7 Guidance for production of hardware. Addresses changes in production environment.
- 6.0 V&V Testing. D0-254 includes Validation testing. Ensures derived requirements make sense and flow back to safety assessment process.

Some Major Differences between D0-254 and D0-178B (Cont.)

- 7.0 Some small differences in CM.
- 8.0 Process Assurance instead of Quality Assurance. Anyone can do PA, doesn’t have to be a QA organization.
- 9.0 Certification liaison in D0-254 not as well defined.
- 10.2 Discusses data packaging to be delivered to certification authority.
  - Considerably more data items to be delivered compared to D0-178B.
- 11.4 Tool Qualification in D0-254 better defined and easier to follow than D0-178B.
- Appendix A. D0-178B, tables A1-A10 focus on processes. D0-254 App. A focuses on the data items.

Figure 2-3

Decision Making Process for Selecting the Hardware Design Assurance Strategy


1
Begin Assessment Process
2
Determine FFP Design Assurance Level
Level A or B
Level D or E
Level C
3
Is Hardware Implementation Simple or Complex?
Simple
Complex
4
Develop Design Assurance Strategy for Level A or Level B Complex FFPs
Modify Strategy
5
Is Strategy Adequate?
No
Yes
6
Document Applicable Fail-Safe Aspects
7
Document Design Assurance Approach
8
Implement Approach

Some significant issues

- Scope. PLD's and ASIC's only? Include Microprocessors?
- Applicability? All Design Assurance Levels?
- What defines "Simple" vs. "Complex" CEH?
- What defines "Comprehensive testing?"
- Application of D0-254 to TSO applications.
- Application of D0-254 to previously TSO'ed equipment that contains CEH.
- What data is relevant to support use of service history for CEH certification credit?

New and Novel Technology Issues

- Merging formerly separate and independent functions on same hardware; multifunction components.
- Displaying critical and non-critical functional paths in same systems/components.
- Replacing mechanical with electronic parts.
- Using CEH in roles “traditionally” targeted at software.
- Configuration control of complex, highly integrated systems.

Appendix A Notes

? Data that should be submitted is indicated by an S in the Submit column. HC1 and HC2 data used for certification that need not be submitted should be available. Refer to Section 7.3

? The objectives listed here are for reference only. Not all objectives may be applicable to all assurance levels.

? If this data is used for certification, then its availability is shown in the table. This data is not always used for certification and may not be required.

? This can be accomplished informally through the certification liaison process for Levels C and D. Documentation can be in the form of meeting minutes and and/or presentation material.

? If the applicant references this data item in required data items, it should be available.

? Only traceability data from requirements to test is needed.

? Test coverage of derived or lower hierarchical requirements is not required.

Appendix B
Additional Activities for Levels A and B

- Functional Failure Path Analysis (FFPA)
  - Method, Data
- Design Assurance Methods for Levels A and B
  - Arch. Mitigation
  - Service Experience
  - Adv. Verif. Methods

Advanced Verification Methods

- Elemental Analysis (bottom-up)
- Safety Specific (top-down)
- Formal Methods (error detection & preclusion)

Other Resources

- FAA Complex Electronic Hardware Interactive Video Training (IVT) - Video and Workbook
- FAA-Contracted UTRC COTS Hardware Report
- DOT/FAA/AR-95/31, “Design, Test, and Certification Issues for Complex Integrated Circuits”
- Company Hardware Design Assurance Standards and Policy

Summary

- AC, Order, and TAD Policy currently in work.
- DO-254 somewhat similar to DO-178B but has some significant differences
- Be proactive, develop and coordinate a strategy, and follow it.
- Questions?